RECEIVED
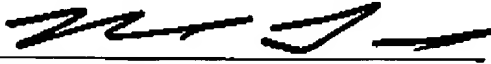CENTRAL FAX CENTER

PATENT   **DEC 0 8 2005**   01AB071 / ALBRP227US

<u>CERTIFICATE OF FACSIMILE TRANSMISSION</u>
I hereby certify that this correspondence (along with any paper referred to as being attached or enclosed) is being faxed to 571-273-8300 on the date shown below to Mail Stop Appeal Brief - Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Date: /2-8-05

Himanshu S. Amin

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re patent application of:

Applicant(s): Brian Alan Batke *et al.* | Examiner: Dustin Nguyen

Serial No: 09/965,267 | Art Unit: 2154

Filing Date: September 27, 2001

Title: ADAPTIVE METHOD FOR DUPLICATIVE IP ADDRESS DETECTION

Mail Stop Appeal Brief – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPEAL BRIEF

Dear Sir:

Appellants' representative submits this brief in connection with an appeal of the above-identified patent application. A credit card payment form is filed concurrently herewith in connection with all fees due regarding this appeal brief. In the event any additional fees may be due and/or are not covered by the credit card, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1063 [ALBRP227US].

I.   Real Party in Interest (37 C.F.R. §41.37(c)(1)(i))

The real party in interest in the present appeal is Rockwell Technologies, LLC, the assignee of the present application.

II.   Related Appeals and Interferences (37 C.F.R. §41.37(c)(1)(ii))

Appellants, appellants' legal representative, and/or the assignee of the present application are not aware of any appeals or interferences which may be related to, will directly affect, or be directly affected by or have a bearing on the Board's decision in the pending appeal.

III.   Status of Claims (37 C.F.R. §41.37(c)(1)(iii))

Claims 1-18 stand rejected by the Examiner. The rejection of claims 1-18 is being appealed.

IV.   Status of Amendments (37 C.F.R. §41.37(c)(1)(iv))

No claim amendments have been entered after the Final Office Action.

V.   Summary of Claimed Subject Matter (37 C.F.R. §41.37(c)(1)(v))

A.   Independent Claim 1

Independent claim 1 recites a method for a probing entity to detect a duplicate IP address, the method comprising: generating an identifying value that identifies a random period of time to wait before probing a network with which a probing entity desires to interact; waiting a random period of time related to the identifying value; sending one or more first ARP probes onto the network with which the probing entity desires to interact; determining whether a response to the first ARP probes indicates that there is a duplicate IP address conflict; determining whether the probing entity is connected to an active network; sending one or more second ARP probes onto the network with which the probing entity desires to interact; and determining whether a response to the second ARP probes indicates that there is a duplicate IP address conflict. (*See e.g.*, pg. 5, ll. 14-24; pg. 9, line 20 – pg. 13, line 2; *See generally* Figs. 12-13).

2

B.   Independent Claim 12

Independent claim 12 recites a computer readable medium storing computer executable instructions operable to perform a method for a probing entity to detect a duplicate IP address, the method comprising: generating an identifying value that identifies a random period of time to wait before probing a network with which a probing entity desires to interact; waiting a random period of time related to the identifying value; sending one or more first ARP probes onto the network with which the probing entity desires to interact; determining whether a response to the first ARP probes indicates that there is a duplicate IP address conflict; determining whether the probing entity is connected to an active network; sending one or more second ARP probes onto the network with which the probing entity desires to interact; and determining whether a response to the second ARP probes indicates that there is a duplicate IP address conflict. (*See e.g.*, pg. 5, line 25 – pg. 6, line 4; pg. 8, line 22 – pg. 9, line 7; pg. 13, line 3 – pg. 16, line 10; *See generally* Figs. 1, 14, and 15).

C.   Independent Claim 15

Independent claim 15 recites a system for detecting and preventing the use of duplicate IP addresses comprising: a random time period generator operable to produce a value representing a period of time that a probing entity should wait before invoking the processing of a probe generator; a probe generator operable to produce an ARP probe; a response analyzer operable to analyze a response to an ARP probe and to determine whether the response to the ARP probe indicates that an IP address associated with the probing entity is a duplicate IP address; and an active network detector operable to determine whether the system is connected to an active network. (*See e.g.*, pg. 3, line 30 – pg. 5, line 13; pg. 8, line 22 – pg. 9, line 7; pg. 13, line 3 – pg. 16, line 10; *See generally* Figs. 1, 14, and 15).

D.   Independent Claim 17

Independent claim 17 recites a computer readable medium storing computer executable components of a system for detecting and preventing the use of duplicate IP

3

addresses, the system comprising: a random time period generating component operable to produce a value representing a period of time that a probing entity should wait before invoking the processing of a probe generator component; a probe generating component operable to produce an ARP probe; a response analyzing component operable to analyze a response to an ARP probe and to determine whether the response to the ARP probe indicates that an IP address associated with the probing entity is a duplicate IP address; and an active network detecting component operable to determine whether the system is connected to an active network. (*See e.g.*, pg. 5, line 25 – pg. 6, line 4; pg. 8, line 22 – pg. 9, line 7; pg. 13, line 3 – pg. 16, line 10; *See generally* Figs. 1, 14, and 15).

E.   Independent Claim 18

Independent claim 18 recites a system for detecting and preventing the use of duplicate IP addresses comprising: means for identifying a random period of time that should be waited before a probe generating means is activated; means for generating an ARP probe; means for distributing the ARP probe to one or more IP components; means for interpreting a response to the ARP probe; and means for determining whether a probing entity is connected to an active network. (*See e.g.*, pg. 6, ll. 5-13; pg. 8, line 22 – pg. 9, line 7; pg. 13, line 3 – pg. 16, line 10; *See generally* Figs. 1, 14, and 15).

VI.   Grounds of Rejection to be Reviewed (37 C.F.R. §41.37(c)(1)(vi))

A.   Claims 1-18 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Cole *et al.* (US 5,854,901), in view of Arndt *et al.* (US 5,724,510).

VII.   Argument (37 C.F.R. §41.37(c)(1)(vii))

A.   Rejection of Claims 1-18 Under 35 U.S.C. §103(a)

Claims 1-18 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Cole *et al.* (US 5,854,901), in view of Arndt *et al.* (US 5,724,510). It is requested that this rejection be reversed for at least the following reason. Cole *et al.* and Arndt *et al.*, alone or in combination, do not teach or suggest all the limitations of the subject claims.

4

To reject claims in an application under §103, an examiner must establish a *prima facie* case of obviousness. A *prima facie* case of obviousness is established by a showing of three basic criteria. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) *must teach or suggest all the claim limitations*. *See* MPEP §706.02(j). The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *See In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

Appellants' claimed invention relates to a system and method of detecting and preventing the use of duplicate IP addresses in order to select and set new IP addresses. (*See* Abstract). In particular, independent claim 1 (and similar independent claims 12, 15, and 17-18) recites *generating an identifying value that identifies a random period of time to wait before probing a network with which a probing entity desires to interact.* Cole *et al.* and Arndt *et al.*, alone or in combination, do not teach or suggest such novel aspect of the invention as claimed.

Cole *et al.* describes a serverless network protocol that discovers IP addresses for network endpoints. (*See* col. 1, ll. 10-12). The Examiner concedes that Cole *et al.* does not specifically disclose *generating an identifying value that identifies a random period of time to wait before probing a network with which a probing entity desires to interact.* (*See* Final Office Action dated August 24, 2005, pages 3-4). In order to cure this deficiency, the Examiner offers Arndt *et al.*

Arndt *et al.* describes a method for configuring valid IP addresses for a LAN test instrument and detecting duplicate IP addresses between devices in a LAN. (*See* col. 1, ll. 7-10). The Examiner contends that Arndt *et al.* discloses generating an identifying value that identifies a random period of time to wait before probing a network with which a probing entity desires to interact at col. 1, ll. 28-34. (*See* Final Office Action dated August 24, 2005, pg. 4). Appellants' representative respectfully disagrees with such

5

contention. At the indicated passage, Arndt *et al.* describes a method that resolves collisions between nodes. When two or more nodes try to send information at the same time, a collision occurs. A "back off" procedure then operates, where each node waits a random period of time before attempting to send the information again. (*See* col. 1, ll. 28-34). Arndt *et al.* therefore performs the "back off" procedure after a collision occurs, not before the network is probed. The invention as claimed, in contrast, identifies a random period of time to wait before the network is probed and thus before a collision could possibly occur. Waiting a random period of time before resending information *after a collision* is not equivalent to identifying a random period of time to wait *before probing a network* as recited in the subject claims.

In response, the Examiner contends that Arndt *et al.* discloses this limitation by monitoring network traffic for a period of time before sending or generating the ARP request to the target address at col. 2, line 55 – col. 3, line 9 and col. 11, ll. 9-18. (*See* Final Office Action dated August 24, 2005, pg. 2). Appellants' representative respectfully disagrees with this contention. The claimed invention identifies a *random* period of time to wait before probing a network, whereas the cited reference describes a test instrument that monitors network traffic for a *predetermined* period of time before choosing an IP address. (*See* col. 2, line 55 – col. 3, line 9 and col. 11, ll. 9-18). Because the identifying value is random, it is likely that a device will wait a different period of time each time it probes a network—such waiting period is not predetermined, but determined for each time a device needs to select an IP address. Arndt *et al.* is silent with respect to generating an identifying value that identifies a *random* period of time to wait before probing a network with which a probing entity desires to interact, as claimed.

In view of at least the foregoing, it is readily apparent that Cole *et al.* and Arndt *et al.*, alone or in combination, do not teach or suggest the invention as recited in independent claims 1, 12, 15, and 17-18 (and associated dependent claims 2-11, 13-14, and 16). Accordingly, this rejection should be reversed.

6

09/965,267   01AB071 / ALBRP227US

B.   Conclusion

For at least the above reasons, the claims currently under consideration are believed to be patentable over the cited references. Accordingly, it is respectfully requested that the rejections of claims 1-18 be reversed.

If any additional fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [ALBRP227US].

Respectfully submitted,

AMIN & TUROCY, LLP

Himanshu S. Amin
Reg. No. 40,894

AMIN & TUROCY, LLP
24th Floor, National City Center
1900 East 9th Street
Cleveland, Ohio 44114
Telephone: (216) 696-8730
Facsimile: (216) 696-8731

7

09/965,267   01AB071 / ALBRP227US

VIII. Claims Appendix (37 C.F.R. §41.37(c)(1)(viii))

1.   A method for a probing entity to detect a duplicate IP address, the method comprising:

generating an identifying value that identifies a random period of time to wait before probing a network with which a probing entity desires to interact;

waiting a random period of time related to the identifying value;

sending one or more first ARP probes onto the network with which the probing entity desires to interact;

determining whether a response to the first ARP probes indicates that there is a duplicate IP address conflict;

determining whether the probing entity is connected to an active network;

sending one or more second ARP probes onto the network with which the probing entity desires to interact; and

determining whether a response to the second ARP probes indicates that there is a duplicate IP address conflict.

2.   The method of claim 1, comprising:

sending ARP probes until the probing entity is connected to an active network.

3.   The method of claim 2, comprising:

not employing the potentially duplicate IP address until after all the processing associated with claim 2 has been completed.

4.   The method of claim 1, the length of the random period of time is generated by examining at least one of a GUID, a physical address, an IP address and a counter.

5.   The method of claim 1, the one or more first ARP probes contain the physical address of the probing entity and a potentially duplicate IP address.

8

6.   The method of claim 5, the response to the first ARP probes contain the physical address of the probing entity, the physical address of a responding entity, the IP address of a responding entity and the potentially duplicate IP address.

7.   The method of claim 6, determining whether a response to the first ARP probes indicates that there is a duplicate IP address conflict comprises comparing the potentially duplicate IP address of the response to the potentially duplicate IP address associated with the probing entity.

8.   The method of claim 7, the one or more second ARP probes contain the physical address of the probing entity and a potentially duplicate IP address.

9.   The method of claim 8, the response to the second ARP probes contain the physical address of the probing entity, the physical address of the responding entity, the IP address of the responding entity and the potentially duplicate IP address.

10.   The method of claim 9, determining whether a response to the second ARP probes indicates that there is a duplicate IP address conflict comprises comparing the potentially duplicate IP address of the response to the potentially duplicate IP address associated with the probing entity.

11.   The method of claim 1, determining whether a probing entity is connected to an active network comprises at least one of analyzing network traffic received by a network interface associated with the probing entity, analyzing electrical signals received from hardware associated with the network with which the probing entity desires to interact, and analyzing BPDUs (Bridge Protocol Data Units) received by a network device associated with the network with which the probing entity desires to interact.

9

12.   A computer readable medium storing computer executable instructions operable
to perform a method for a probing entity to detect a duplicate IP address, the method
comprising:

generating an identifying value that identifies a random period of time to wait
before probing a network with which a probing entity desires to interact;

waiting a random period of time related to the identifying value;

sending one or more first ARP probes onto the network with which the probing
entity desires to interact;

determining whether a response to the first ARP probes indicates that there is a
duplicate IP address conflict;

determining whether the probing entity is connected to an active network;

sending one or more second ARP probes onto the network with which the probing
entity desires to interact; and

determining whether a response to the second ARP probes indicates that there is a
duplicate IP address conflict.

13.   The computer readable medium of claim 12, the method further comprises:
sending ARP probes until the probing entity is connected to an active network.

14.   The computer readable medium of claim 13, the method further comprises:
not employing the potentially duplicate IP address until after all the processing
associated with claim 13 has been completed.

10

15.   A system for detecting and preventing the use of duplicate IP addresses comprising:

a random time period generator operable to produce a value representing a period of time that a probing entity should wait before invoking the processing of a probe generator;

a probe generator operable to produce an ARP probe;

a response analyzer operable to analyze a response to an ARP probe and to determine whether the response to the ARP probe indicates that an IP address associated with the probing entity is a duplicate IP address; and

an active network detector operable to determine whether the system is connected to an active network.

16.   The system of claim 15, the active network detector comprises at least one of: a network traffic analyzer operable to analyze network traffic and to determine whether the probing entity is connected to an active network, a network pulse analyzer operable to analyze one or more electrical signals received from network devices operably connected to the probing entity and to determine whether the probing entity is connected to an active network, and a BPDU analyzer operable to analyze one or more bridge protocol data units received by network devices operably connected to the probing entity and to determine whether the probing entity is connected to an active network.

17.   A computer readable medium storing computer executable components of a system for detecting and preventing the use of duplicate IP addresses, the system comprising:

a random time period generating component operable to produce a value representing a period of time that a probing entity should wait before invoking the processing of a probe generator component;

a probe generating component operable to produce an ARP probe;

a response analyzing component operable to analyze a response to an ARP probe and to determine whether the response to the ARP probe indicates that an IP address associated with the probing entity is a duplicate IP address; and

an active network detecting component operable to determine whether the system is connected to an active network.

18.   A system for detecting and preventing the use of duplicate IP addresses comprising:

means for identifying a random period of time that should be waited before a probe generating means is activated;

means for generating an ARP probe;

means for distributing the ARP probe to one or more IP components;

means for interpreting a response to the ARP probe; and

means for determining whether a probing entity is connected to an active network.

IX.   Evidence Appendix (37 C.F.R. §41.37(c)(1)(ix))

None.

X.   Related Proceedings Appendix (37 C.F.R. §41.37(c)(1)(x))

None.

12